IDENTITY THEFT IDENTITY THEFT IDENTITY THEFT

IF SOMEONE IS USING YOUR IDENTIFYING INFORMATION (NAME, DATE OF BIRTH, SOCIAL SECURITY NUMBER, DRIVERS LICENSE NUMBER, ETC.) TO OBTAIN GOODS, SERVICES, CREDIT AND/OR OPEN FRAUDULENT BANK ACCOUNTS...

YOU ARE A VICTIM OF IDENTITY THEFT!

Identity Theft—A Growing Concern

Each year identity theft - one of the fastest growing types of fraud, harms thousands of citizens throughout our state. Ultimately, the identity thief hopes to obtain personal information about you - your social security number, birth name, credit card numbers, or birth date. With this information, imposters can assume your identity and establish bank accounts or line of credits with financial institutions in your name, leaving you to deal with the fallout. The identity thief can also pose as you in the commission of a crime, perhaps leaving you with a false criminal record.

Identity Theft Statistics

- Identity theft is the fastest growing crime in the United States.
- Washington state ranks 8th in the nation in identity theft crimes per capita.
- The Federal Trade Commission (FTC) found that complaints of identity theft increased 87 percent between 2001 and 2002, and over 161,000 complaints were received by the agency last year.
- A July 2003 study by Gartner, Inc. found that there was a 79 percent increase in identity theft in the past year alone.
- The U.S. Secret Service has estimated that consumers nationwide lose \$745 million to identity theft each year.

Contact Information

Major Credit Bureaus:

Equifax

P.O. BOX 740241 Atlanta, GA. 30374-0241 (800) 685-1111 www.equifax.com

Experian

P.O. BOX 1017 Allen, TX. 75013-1017 (888) 397-3742 www.experian.com

Trans Union

P.O. BOX 6790 Fullerton, CA. 92834-6790 (800) 925-8800 www.transunion.com

Remember, if you have been the victim of credit fraud or denied credit, you are entitled to a free credit report. If you are a victim of fraud, be sure to ask the credit bureaus for free copies.

Duvall-Carnation Police Department

Report Identity Theft CALL 911

Duvall Police Department 26225 NE Stephens Street Duvall, WA 98019

Police Business Number

(425) 788-1519

Social Security Administration

Report Fraud: (800) 269-0271

Write:

SSA Fraud Hotline, PO BOX 17768, Baltimore, NY. 21235

Other Helpful Resources:

Federal Trade Commission: (877) FTC-HELP for help in

any type of consumer complaint.

FTC Homepage: www.consumer.gov/idtheft



DUVALL-CARNATION POLICE

IDENTITY THEFT GUIDE

http://duvallwa.gov/departments/police.html



Duvall-Carnation Police Department 26225 NE Stephens Street Duvall, WA 98019 (425) 788-1519

What is it?

Identity theft is a crime. The term identity theft refers to a type of crime in which someone wrongfully obtains and uses another persons personal data in some way that involves fraud or deception, typically for economic gain. In most cases, your personal information such as your name, date of birth, Social security number, bank account or credit card number, or other valuable identifying data can be used, if they fall into the wrong hands, to personally profit at your expenses. Some cases have shown that someone's entire identity had been taken and they fell subject to substantial financial losses and emotional distress.

How does it happen?

There are many ways to fall victim to identity theft, and unfortunately it does not take someone breaking into your home to get your information. One of the common ways criminals get your personal information in



called 'shoulder surfing'. They may watch you from nearby or listen in on your conversation while you are in a public setting. Typically, they will listen while you give a credit card number over the phone, or watch as you enter your card number onto a computer.

The area near your home may not be as secure as you might think. The second most common tactic used to obtain your personal information is called 'dumpster diving'. Criminals will go through your garbage or a community dumpster to get copies of you checks, credit card or bank statements, or other documents that might include your name, address, and phone number. When they get this type of information, it is easier for them to control your identity.

Another very common criminal practice is 'mail theft'. In these cases, they will take the mail directly from your mailbox in an attempt to get your personal information. This type of crime happens frequently, but it is very prevalent during the holiday season. Criminals will look for credit card applications to try to open accounts under your name. This also occurs during dumpster diving also. It is a good practice to shred or tear up the applications if they are not going to be used.

Finally, be careful what you respond to on your computer. E-mail has become the newest communication highway and unfortunately, there are some sophisticated criminals.

The 'SPAM' that you may get via email might be a subtle request from a criminal soliciting a response from you in an attempt to get your personal information or credit numbers. The

'SPAM' might promise you some benefit or ask for financial assistance to an organization, and there is no intention of doing this. They are just suckering you in.

These are just examples of how quickly your identity can be taken from you. Criminals will use this information almost immediately after getting it, and the financial damage they inflict will generally happen long before the victim even realizes it.

How can I protect myself?

The Federal Government has recognized the severity of identity theft and had developed a simple system to help people from falling victim. Remember the word 'SCAM'

- S- Be stingy about giving out your personal information to others unless you have reason to trust them, regardless of where you are. Adopt a "need-to-know" approach to your personal data.
- <u>C-</u> <u>Check</u> your financial information regularly and look for what should be there and what shouldn't.
- A- Ask periodically for a copy of your credit report.
- <u>M-</u> Maintain careful records of your banking and financial history.

Unfortunately, even if you follow these steps, you may still fall victim to this crime.

What should I do if I've become a victim of Identity Theft?

If you think you have fallen victim to the crime of identity theft, act immediately to minimize the damage to your finances and your reputation. Here are some actions to take right away:

1. Contact your creditors and obtain current account status records showing transactions.

- 2. Contact your local police agency for guidance, or a case number if the offense occurred in the local jurisdiction. (Most creditors will need a police case number for monetary reimbursement)
- 3. Contact the Federal Trade Commission (FTC) to report the situation. 1-877-ID THEFT.

Keep your computer and its contents safe

Computer technology makes it easier for criminals to find personal and financial information. If you keep credit card numbers, account numbers, and tax information in your system or use e-mail to do financial business, take steps to make sure that this information is safe from hackers and thieves. The following measures can help protect against identity theft online.

- Protect your computer, including laptops, with a startup password that is a combination of letters (upper and lower case), numbers and symbols.
 Don't use an automatic login feature that saves your user name and password.
- Disable file-sharing software to prevent unauthorized access to your computer and its data.
- Install virus protection software and be sure to update it regularly. Viruses can instruct your computer to send information to other systems without your knowledge.
- Be careful what you open. E-mails from strangers could contain viruses or programs to hijack your Internet connection or damage your computer.
- Don't send personal or confidential information over e-mail. E-mail messages are not secure.

Shop and bank safely online:

- Before giving your credit card number or other financial information to a business, make sure that the merchant has a secure transaction system. Most Internet browsers indicate when you are using a secure Internet link. To check to see if a Web site is secure look for:
 - A Web site address that starts with https://, or
 - An icon, often a lock or an unbroken key, at the bottom right corner of the screen.
- Fake or "spoof" Web sites are designed to trick consumers and collect their personal information. Be cautious when clicking on a link or an unknown Web site or unfamiliar e-mail. The link may take you to a fraudulent site.